– Sonderveröffentlichung –

CYBERKRIMINALITÄT – SO KÖNNEN SIE SICH SCHÜTZEN

© ISTOCK.COM/ANYABERKUT

BETRUGSVERSUCH **IM INTERNET**

Gefahr Identitätsdiebstahl

Bewusster Umgang mit privaten Daten – sowohl analog als auch digital

Von Frank Beckenbach

Göttingen. Der gute Ruf ist weg und vielfach auch viel Geld, wenn sich „Identitätsdiebe“ im Internet für jemand anderes ausgeben. Mit illegal erworbenen Login-Daten, die beispielsweise von gecrackten Handelsplattformen stammen, shoppen Kriminelle dank dieses Identitätsdiebstahls auf fremde Rechnung, betteln unter Umständen sogar bei Ihren Bekannten um finanzielle Unterstützung oder posten unschöne Dinge in fremdem Namen. Daraus kann sich für den Betroffenen ein wahrer Alptraum entwickeln.

Was passiert bei so einem Identitätsdiebstahl? Die Täter nutzen gestohlene Daten, um im Internet Waren auf fremde Rechnung zu bestellen oder sie schließen kostenpflichtige Verträge ab. Dazu benötigen die Täter in Einzelfällen nur einen Namen und die zugehörige Kontonummer fürs Online-Shopping.

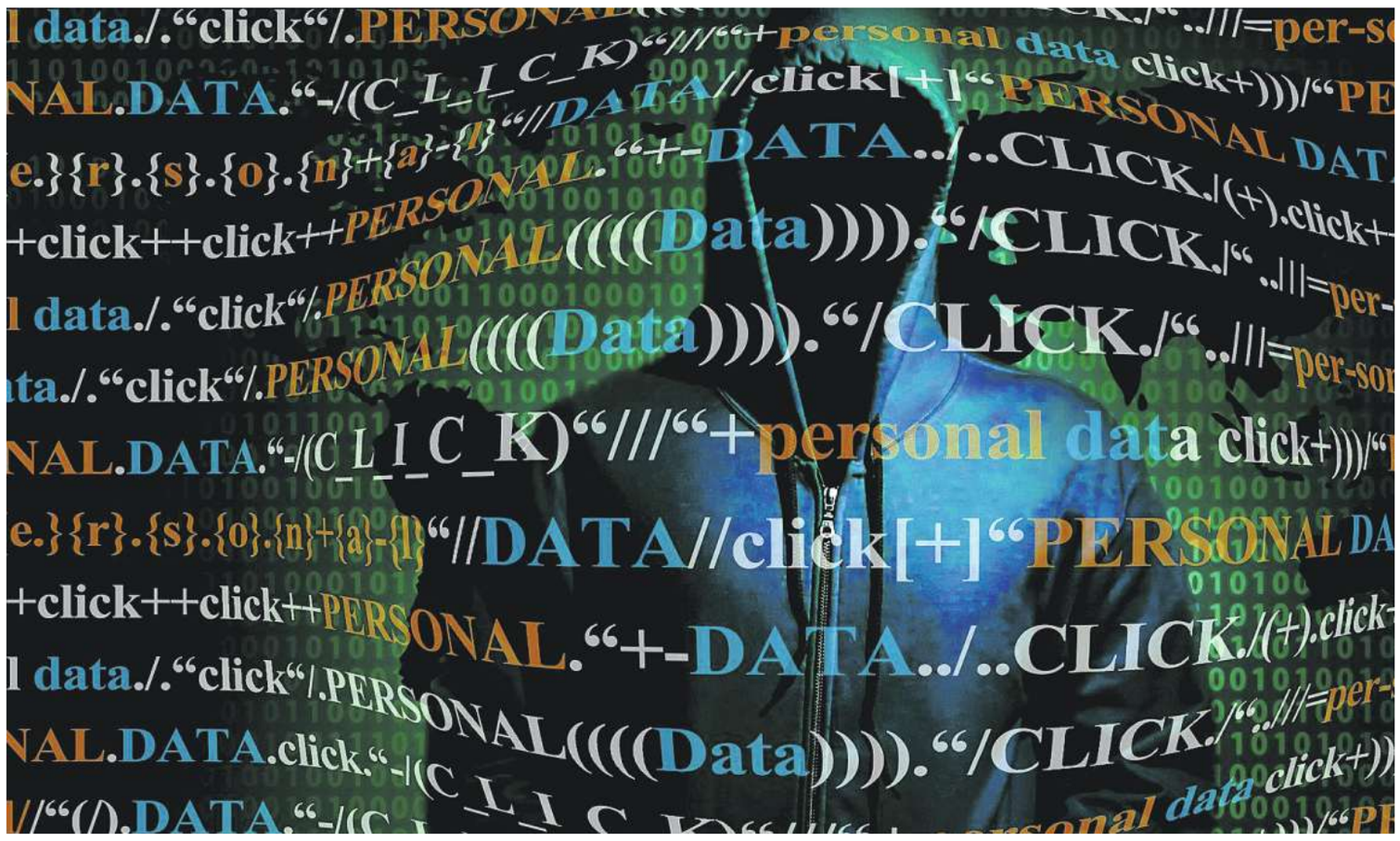
Häufig tritt auch ein weiterer Trick auf, der mit dem Enkeltrick Parallelen aufweist. Unter Vorspiegelung einer Notlage melden sich diese Trickbetrüger bei Bekannten und bitten um Geld, die Social-Media-Plattformen machen es möglich, herauszufinden, wer wem nahe steht.

Aber nicht immer verfolgen Hacker ausschließlich finanzielle Motive, sondern verwenden die fremden Identitäten für Cyber-Mobbing oder Rufschädigung im Netz. Und das Netz, das hat sich schon vielfach herausgestellt, es vergisst nicht so schnell.

Ein Identitätsdiebstahl, auch Identitätsmissbrauch oder Identitätsbetrug genannt, liegt immer dann vor, wenn Dritte die Daten einer anderen Person nutzen und damit Straftaten begehen. Kurz gesagt: Identitätsdiebstahl ist Datenklau für unterschiedlichste Formen von Onlinebetrug.

Christian Kalinowski, Kriminalhauptkommissar der Polizeidirektion Göttingen und Mitglied der Task Force Cybercrime, warnt: „In der Regel sind Identitätsdiebstähle mit dem Ziel verbunden, mit der erlangten Identität weitere Straftaten zu begehen.“ Und: „Cyberkriminelle passen ihr Handeln immer wieder den aktuellen Lebensumständen an und nutzen Gewohnheiten ihrer Opfer aus. Dabei setzen sie nach wie vor auf „Social Engineering“ als bevorzugte Methode, um an Daten oder das Geld ihrer Opfer zu gelangen. Da die Täter sich immer wieder neu anpassten und ihr Handeln derart professionell sei, sei es für viele Menschen schwer, zu erkennen, dass sie gerade Opfer einer Straftat werden, sagt Kalinowski.

Die Spezialisten der Sparkassen Göttingen und Duderstadt, der VR-Banken Mitte und Südniedersachsen, der Volksbank Kassel Göttingen sowie der Vorsitzende des Vereins für Cybersicherheit e.V. geben nun wertvolle Tipps rund um das Thema Identitätsdiebstahl.



SYMBOLFOTO: PIXABAY

Christian Kalinowski, Kriminalhauptkommissar der Polizeidirektion Göttingen und Mitglied der Task Force Cybercrime. FOTO: PRIVAT

JAN DANIEL BREMER

VR-BANK IN SÜDNIEDERSACHSEN

„Erhält ein Betrugsopfer Rechnungen, sollten diese zusammen mit der Bank geprüft werden. Je nach Bezahlart bestehen verschiedene Möglichkeiten. Zum Beispiel können Lastschriften wegen Widerspruchs zurückgegeben werden. Bei der Belastung eines Kreditkartenkontos kann dieses gesperrt werden“, sagt Jan Daniel Bremer, Business Administrator der VR-Bank Südniedersachsen. „Im schlimmsten Fall muss ein Konto geschlossen und ein neues (mit einer neuen IBAN) errichtet werden.“ Wichtig sei, dass der Lieferant der Waren bei einem Identitätsdiebstahl im guten Glauben geliefert hat, so dass sich ihm gegenüber keine Ansätze ergeben. Eine Strafanzeige bei der Polizei sollte auf jeden Fall gestellt werden, denn man müsse von einer Vielzahl einzelner Betrugsvorgänge bei einem Opfer ausgehen. „Letztendlich muss mit negativen Schufa-Einträgen gerechnet werden. Dies schädigt dann die Bonität des Kunden insgesamt.“

MARCEL WAGENER

SPARKASSE GÖTTINGEN

„In der Regel kann nicht mit Sicherheit festgestellt werden, aus welcher Quelle die entwendeten Identitätsdaten stammen, in welchem Umfang die Daten den Tätern tatsächlich vorliegen und zu welchem Zeitpunkt der Diebstahl begangen wurde“, sagt Marcel Wagener, zuständig für Bezahlverfahren bei der Sparkasse Göttingen. „Es kann grundsätzlich möglich sein, dass die Täter auf demselben Weg, über den sie an die Identitätsdaten gelangt sind – beispielsweise über Trojaner, Phishing-Mails, etc. – auch in den Besitz von Online-Banking-Zugangsdaten und der IBAN oder Kreditkartennummer des Kunden gekommen sind. Aus diesem Grund ist es immer ratsam, nach einem solchen Vorfall die Online-Banking-Zugangsdaten, also Anmeldename und PIN, zu ändern und die Abbuchungen auf dem Girokonto und der Kreditkarte im Auge zu behalten.“

ANNETTE BÖHLE

VOLKSBANK KASSEL GÖTTINGEN

„Durch einen Vermögensschaden kann möglicherweise die Liquidität des Kunden beeinträchtigt werden“, warnt Annette Böhle, Abteilungsleiterin Zahlungsverkehr der Volksbank Kassel Göttingen. „Gefakte Internetkäufe ziehen unbezahlte Rechnungen und Mahnungen nach sich und verursachen negative Einträge in den Bonitätsakten von SCHUFA und Co. Das kann den Bonitätsscore extrem verschlechtern. In der Folge können sich Kreditkartensperren anschließen, ein Rechnungskauf oder Ratenkauf kann abgelehnt werden“, sagt Böhle.

DANIEL ZÖPFGEN

SPARKASSE DUDERSTADT

„Da in diesen Fällen den Betrügern persönliche Daten der Opfer bekannt sind, werden die Betrüger möglicherweise versuchen, sich der Bank gegenüber als echter Kontoinhaber auszugeben. Um Schäden zu verhindern, sollte auch die jeweilige Bank informiert werden“, sagt Daniel Zöpfgen, Fachberater für Giro- und Zahlungsverkehr der Sparkasse Duderstadt. Mit den ergaunerten Identitätsdaten könnten Waren bestellt werden oder es kann versucht werden, Konten betrügerisch zu eröffnen. Wenn beispielsweise eine von den Betrügern bestellte Ware nicht bezahlt wird oder die betrügerisch auf den Namen der Opfer lautenden Konten missbraucht werden, kann das zu negativen Schufa-Einträgen führen. „Diese haben dann Einfluss auf die Bonitätsbewertung durch das Kreditinstitut. Das gilt übrigens auch für Versandhäuser oder Händler, die mit der Schufa zusammenarbeiten“, sagt Zöpfgen.

UWE LÜHRIG

VEREIN FÜR CYBERSICHERHEIT NIEDERSACHSEN

„Den meisten Tätern geht es darum, an digitale Identitäten heranzukommen, um damit weitere Straftaten (beispielsweise Betrugs- oder Erpressungshandlungen) begehen zu können. Dafür setzen Cyberkriminelle auch heute noch auf altbekannte Maleware, allen voran Spam-Mail-Kampagnen und professionelle Phishing-Mails mit maliziösen Office-Anhängen oder dementsprechende Verlinkungen“, sagt Uwe Lührig, 1. Vorsitzender des Vereins für Cyber-Sicherheit Niedersachsen e.V.. „Diese Ransomware gehört zu den häufigsten und gefährlichsten Typen von Schadsoftware. Mittlerweile können Baukästen im sogenannten Darknet erworben werden, sodass auch technisch nicht so versierte Kriminelle in der digitalen Welt tätig werden können. Dazu werden entweder gestohlene, aber real-existierende E-Mail-Accounts im Darknet erworben oder die Sozialen Netzwerke gezielt nach persönlichen Informationen wie Name, Vorname, Geburtsdatum, Handynummer oder E-Mail-Adresse durchsucht. Sind aktuelle Informationen im Netz verbreitet, lassen sich individuelle Phishing-Mails generieren, um so mögliche Opfer gezielt angreifen zu können. Ich will aber auch darauf hinweisen, dass solche Angriffe nicht nur per E-Mail erfolgen, sondern ebenfalls über SMS-Nachrichten durchgeführt werden.“

FLORIAN HARTLEIB

VR-BANK MITTE

„Betrüger bestellen auf den Namen des Opfers Waren oder Dienstleistungen und zahlen die Rechnungen nicht. Nicht bezahlte Rechnungen führen zu negativen Einträgen in der Schufa, die die Bonität verschlechtern. Daher sollten Kunden mit ihrem Ansprechpartner in der Bank intensiv prüfen, welche Auswirkungen individuell vorherrschen.“, sagt Florian Hartleib, Prokurist der VR-Bank Mitte.

Cloudrelevante Sicherheitslösungen

Wenig Know-How bei kleinen und mittelständischen Unternehmen

Eine digitale Strategie zu entwickeln, die passgenau die Anforderungen und Wünsche eines Unternehmens abdeckt und diese dann auch umzusetzen, das ist die Aufgabe, der sich der IT-Dienstleisters Arineo täglich stellt. So entstehen IT-Strategien, mit der Unternehmen die Wettbewerbsfähigkeit steigern und ihre Unternehmensziele besser realisieren können. Das Göttinger Unternehmen unterstützt Firmen bei der Digitalisierung und der Automatisierung, natürlich nicht ohne die Daten-Sicherheit im Rahmen dieser Strategie zu vernachlässigen. „Wir fokussieren uns auf cloudbasierte Unternehmenslösungen. Hier beraten wir nicht nur die Software-Lösungen, sondern auch die cloudrelevanten Sicherheitslösungen – fokussiert auf die Angebote von Microsoft und SAP“, sagt Arineo-Geschäftsführer Frank Wilkes.

Vielfach verfügten kleine und mittelständische Unternehmen nicht über die Möglichkeiten, diese Sicherheitfeatures selbst bereitzustellen, haben die IT-Spezialisten feststellen müssen. „Einerseits fehlt das Know-How und andererseits sind die damit verbundenen Kosten zu hoch“, sagt Wilkes. Heute sei es möglich, diese sicheren Lösungen als Komplettangebot von einem Dienstleister zu beziehen, inklusive aller Sicherheitsfeatures.